What Is Claimed Is:

1. A system comprising:

an operating system adapted to operate on a processor;

a memory device having a protected area, wherein said protected area is not directly accessible to said operating system;

firmware coupled to said memory device;

a virtual machine manager installed in said firmware operative to provide said operating system access to said protected area independently of any memory device controller.

2. The system of claim 1, further comprising a plurality of protected areas on said memory device.

3. The system of claim 1, wherein said memory device comprises a hard disk.

4. The system of claim 2, wherein said system functions as a redundant array of independent disks (RAID).

5. The system of claim 1, further comprising a known working configuration stored in said protected area, wherein said known working configuration comprises critical file-system structures.

6. The system of claim 1, wherein said firmware provides operating system-specific file-system support.

7. The system of claim 1, further comprising extensibility modules stored in said protected area for pre-boot support.

8. The system of claim 1, wherein said firmware provides operating system-independent file-system support.

9. A method comprising:

(a) protecting an area on a memory device;

(b) providing a virtual machine manager (VMM) in firmware coupled to said memory device; and

(c) providing access to said protected area through said VMM independently of any memory device controller.

10. The method of claim 9, wherein (c) further comprises:

proxying an access request for said protected area with said VMM; and

executing said access request to said protected area with said VMM.

11. The method of claim 9, wherein (a) further comprises protecting a plurality of areas on said memory device.

12. The method of claim 11, further comprising

(d) using said plurality of protected areas as a redundant array of independent disks (RAID).

13. The method of claim 12, wherein (c) further comprises:

translating a logical block address (LBA) request for said RAID to said plurality of protected areas; and

executing said LBA request.

14. The method of claim 9, further comprising:

(d) storing a known working configuration in said protected area, wherein said known working configuration comprises critical file-system structures; and

(e) using said known working configuration when a computer adapted to execute said method is unable to boot properly.

15. The method of claim 9, further comprising:

(d) providing operating system-specific file-system support with said firmware.

16. The method of claim 9, further comprising:

(d) storing extensibility modules in said protected area for pre-boot support.

17. The method of claim 9, further comprising:

(d) providing operating system-independent file-system support with said firmware.

18. A machine-accessible medium containing code that, when executed by a computing platform, causes the computing platform to perform a method comprising:

(a) protecting an area on a memory device;

(b) using a virtual machine manager (VMM) coupled to said memory device; and

(c) providing access to said protected area through said VMM independently of any memory device controller.

19. The machine-accessible medium of claim 18, wherein (c) further comprises:

proxying an access request for said protected area with said VMM; and

executing said access request to said protected area with said VMM.

20. The machine-accessible medium of claim 18, wherein (a) further comprises reserving a plurality of areas on said memory device.

21. The machine-accessible medium of claim 20, further containing code that, when executed by a computing platform, causes said method to further comprise:

(d) using said plurality of protected areas as a redundant array of independent disks (RAID).

22. The machine-accessible medium of claim 21, wherein (c) further comprises:

translating a logical block address (LBA) request for said RAID to said protected areas; and

executing said LBA request.

23. The machine-accessible medium of claim 18, further containing code that, when executed by a computing platform, causes said method to further comprise:

(d) storing a known working configuration in said protected area, wherein said known working configuration comprises critical file-system structures; and

(e) using said known working configuration when the computing platform is unable to boot properly.

24. The machine-accessible medium of claim 18, further containing code that, when executed by a computing platform, causes said method to further comprise:

(d) providing operating system-specific file-system support with said firmware.

25. The machine-accessible medium of claim 18, further containing code that, when executed by a computing platform, causes said method to further comprise:

(d) storing extensibility modules in said protected area for pre-boot support.

26. The machine-accessible medium of claim 18, further containing code that, when executed by a computing platform, causes said method to further comprise:

(d) providing operating system-independent file-system support with said firmware.